



H29

"Express Mail" Label No. EV32576561245
Date of Deposit 12-22-03

PATENT
Attorney Docket No.: 040048-000100US

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Address" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By Nina L. McNeill
Nina L. McNeill

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re application of:

Paul Charles Turgeon

Application No.: 09/394,143

Filed: September 10, 1999

For: SYSTEM AND METHOD FOR
PROVIDING SECURE SERVICES
OVER PUBLIC AND PRIVATE
NETWORKS USING A REMOVABLE,
PORTABLE COMPUTER-READABLE
STORAGE MEDIUM AT A NETWORK
ACCESS DEVICE

Examiner: Calvin L. Hewitt II

Art Unit: 3621

APPELLANT BRIEF UNDER 37 CFR
§1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

RECEIVED
JAN 05 2004
GROUP 3600

Appellant offers this Brief in support of the Notice of Appeal mailed concurrently. This Brief is submitted in triplicate as required by 37 CFR §1.192(a).

1. Real Parties in Interest

The real party in interest is NYCE Corporation.

2. Related Appeals and Interferences

No other appeals or interferences are known that will directly affect, are directly affected by, or have a bearing on the Board decision in this appeal.

3. Status of Claims

Claims 1 – 25 are currently pending in the application, which is a Continued Prosecution Application. All pending claims stand finally rejected by the Examiner. The independent claims, i.e. Claims 1 and 17, were amended as part of a Response to an Office Action mailed on July 2, 2003 (paper no. 25, referred to herein as “the Final Office Action”), which reopened prosecution in response to filing of an earlier Appeal Brief. Certain amendments had previously been made to dependent Claims 3 and 9 – 11, and Claims 26 – 28 were previously canceled.

The rejections of Claims 1 – 25 are believed to be improper and are the subject of this appeal. A copy of Claims 1 – 25 as finally rejected is attached as an Appendix.

4. Status of Amendments

No amendments have been filed subsequent to the most recent rejection, mailed September 24, 2003.

5. Summary of the Invention

In one embodiment, the claimed invention relates to methods and systems for providing secure financial services over public communication lines, such as the Internet or other network (Application, p. 4, ll. 22 – 24). The secure financial services are provided by using encrypted information on a portable storage medium, such as a CD (*id.*, p. 4, ll. 24). With this arrangement, the portable storage medium may effectively act as a debit card, allowing a customer holder of the portable storage medium to execute debit transactions electronically (*id.*, p. 4, ll. 24 – 26). The portable storage medium includes information that is typically found on the magnetic strip of conventional plastic debit card, such as the customer's name, account routing number, and the like (*id.*, p. 4, l. 26 – p. 5, l. 2). Like conventional debit cards, transactions using the portable storage medium are enabled with a network that includes accounts at multiple financial institutions for customers whose accounts may be maintained at different financial institutions. No changes are needed to existing debit-network online processing systems to access the accounts (*id.*, p. 10, l. 25 – p. 11, l. 1).

While the information from the magnetic strip of a conventional debit card is readable by any magnetic-strip reader, the information is encrypted on the portable storage medium of the invention (*id.*, p. 5, l. 23 – 25). The holders of such portable storage media are assigned an electronic PIN that may be used in accordance with embodiments of the invention to resolve the conventional PIN used in debit transactions (*id.*, p. 6, ll. 1 – 3). In this way, the card information may remain secure even when transmitted over the Internet or other network (*id.*, p. 6, ll. 14 – 15). This differs from a conventional debit card, whose security relies primarily on the security of the card itself and the conventional PIN, reflecting the fact that conventional debit transactions are not subject to potential interception over public communication lines. In addition to this encrypted information, the portable storage media may include personalized unencrypted information used in providing a greeting, advertising, and the like to the customer when the electronic debit card is used (*id.*, p. 12, ll. 16 – 20).

Use of these methods and systems is illustrated in the application with the example of an Internet debit transaction conducted at a merchant web site, although there may be other uses. In such a transaction, the customer may make payment by inserting the portable storage medium into a network access device, *e.g.* by inserting the electronic debit card into a CD drive of a personal computer, and entering his electronic PIN (*id.*, p. 6, ll. 23 – 24). The encrypted information is transmitted with the electronic PIN to a module on the merchant's web site (*id.*, p. 6, ll. 25 – 26). This module establishes a secure connection with a decryption interface, which forwards a *re*-encrypted PIN to one of the networked financial institutions to seek an approval or denial code (*id.*, p. 7, ll. 2 – 7). This backend seeking of an approval code may be similar to a traditional debit transaction using an existing secure financial network (*id.*, p. 13, l. 23 – p. 14, l. 1) so that, if approved, funds are debited directly from the customer's account (*id.*, p. 14, ll. 3 – 5). The transaction at the merchant web site may be completed (or not) when the approval (or denial) code is returned to that site (*id.*, p. 14, l. 17 – p. 15, l. 5).

6. Issues

Issue 1: Whether under 35 U.S.C. §103(a) Claims 1 – 4, 9 – 12, 17 – 23, and 25 are unpatentable over U.S. Pat. No. 5,771,291 issued to Newton *et al.* (hereinafter “Newtor”) in view of U.S. Pat. No. 6,173,269 issued to Solokl *et al.* (hereinafter “Solokl”). Section 4 beginning on page 3 of the Final Office Action describes the Examiner's position on this issue.

Issue 2: Whether under 35 U.S.C. §103(a) Claims 5 – 8 are unpatentable over Newton and Solokl further in view of U.S. Pat. No. 5,371,797 issued to Bocinsky (hereinafter “Bocinsky”). Section 5 beginning on page 5 of the Final Office Action describes the Examiner's position on this issue.

Issue 3: Whether under 35 U.S.C. §103(a) Claims 13¹ – 16 and 24 are patentable over Newton and Solokl further in viwe of U.S. Pat. No. 4,259,720 (hereinafter “Campbell”). Section 6 beginning on page 6 of the Final Office Action describes the Examiner’s position on this issue.

7. Grouping of the Claims

For purposes of this appeal, the claims are grouped as follows. Group 1 pertains to Issues 1 and 3, and Group 2 pertains to Issue 2.

Group 1: Claims 1 – 4 and 9 – 25.

Group 2: Claim 5 – 8.

Although certain claims are grouped above, Appellant reserves the right outside the context of this appeal to argue independent patentability of any grouped claims.

8. Argument

I. Group 1: Patentability of Claims 1 – 4 and 9 – 25

To support a rejection under 35 U.S.C. §103, the Examiner is charged with factually supporting a *prima facie* case of obviousness. Manual of Patent Examining Procedure, Eighth Edition, First Revision, February, 2003 (hereinafter “MPEP”) 2142. Such a *prima facie* case requires, *inter alia*, that all limitations of the claims be taught or suggested by the cited reference(s) and that there be some suggestion or motivation to

¹ Although Claim 13 stands finally rejected, the Final Office Action does not articulate a specific basis for the rejection. Based on the specific remarks made, Appellant believes the Examiner intended the detailed remarks identified as applicable to Claims 14 – 16 and 24 also to apply to Claim 13. This inference was

combine or modify the reference teachings as the Examiner proposes. MPEP 2143. The rejections of the claims of Group 1 are deficient in at least both these respects.

The claims of Group 1 include the two pending independent claims, Claims 1 and 17, which both require that the claimed invention be applicable across a plurality of financial institutions. In particular, the claimed invention permits a customer holder of a portable storage medium such as a CD to execute debit transactions electronically (Application, p. 4, ll. 24 – 26). These debit transactions may be executed by accessing the customer's financial account at the financial institution where it is maintained, and this capability is provided to multiple customers whose accounts may be maintained at different financial institutions. The finally rejected claims specifically recite that at least some of the financial accounts are maintained at different financial institutions and that each of the plurality of customers may access his account at those different institutions, in accordance with the claim limitations.²

This is completely different from the disclosure of Solokl, which uses an architecture that relies fundamentally on the inclusion of a “service partner bank” (designated 18) and a “service financial institution” (designated 20) that act collectively as an intermediary to coordinate transactions. In order for the system described in Solokl to function, anyone who wishes to perform electronic transactions must have an account at the service partner bank, which provides the funds support for transactions that are effected (“Before a teen ... can enter into a transaction with a merchant using the

noted by Appellants in the response to the previous Office Action, but the Examiner has neither confirmed nor disputed this inference.

² In the Final Office Action, the Examiner apparently gave no weight to those limitations that require application over a plurality of financial institutions “because the recitation occurs in the preamble” (Final Office Action, p. 2, ¶2). This position is a mischaracterization of the amendments that were made in response to the preceding Office Action. Those amendments were made both in the claim body and preamble in such fashion that the body depends on the recitation of the preamble for completeness in describing how the invention applies across a plurality of financial institutions. Furthermore, the language added to the preamble, namely that “at least some of said financial accounts being maintained at different ones of said financial institutions” is not correctly characterized as “merely reciting [a] purpose ... or ... intended use” (Final Office Action, p. 2, ¶2). That language is instead “necessary to give life, meaning, and vitality” to the limitations in the body of the claim that express applicability across a plurality of financial institutions. *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 51 USPQ2d 1161, 1165-66 (Fed. Cir. 1999).

invention, it is first *necessary* that an account be established with the service,” *id.*, Col. 4, ll. 12 – 15, emphasis added; *see also id.*, Col. 5, ll. 47 – 49). All transactions described in Solokl are thus ultimately supported by funds in the service partner bank. The teachings in Solokl even go so far as to suggest that all the funds for the customers be commingled in a single *account*, with database records being used to control access (*id.*, Col. 7, ll. 7 – 12). There is no mechanism disclosed by which an individual may access an account at a different financial institution through the ACH network. This is illustrated by the fact that even if someone already has an existing savings, checking, or similar account at another financial institution, it is necessary that deposits be made to the account at the service partner bank either directly or from those other accounts (*id.*, Col. 4, ll. 30 – 34).

The narrow scope of Solokl as providing ways of supporting transactions with a *single, specific* service partner bank is further illustrated with the description of the virtual automatic teller machine described in connection with Fig. 2 and cited in the Final Office Action at ¶4 to support the rejections:

FIG. 2 is a flow diagram showing the operation of a virtual automatic teller machine (VATM) to execute electronic commercial transactions with teens according to the invention. The VATM provides an account that appears to be a standard bank account for purposes of a transaction, such that an ATM-type exchange may occur. When a teen is logged into his service account he may access the VATM or do other activities, such as read about special offers, check on bonuses, or reconfigure his profile. At the completion of such activities, the teen returns to the user page of the service.

If the teen is accessing his VATM account, he first enters his pass phrase which is verified by checking the user database. The pass phrase is converted to a standard four digit PIN and the service initiates contact with the service financial institution via the ACH network. If contact cannot be initiated, the ATM is exited. Otherwise, the ATM screen is displayed to the teen and the teen may proceed with a transaction, such as balance inquiry or making a purchase.

(*Id.*, Col. 7, l. 60 – Col. 8, l. 12, emphasis added, reference numbers omitted).

As described, the virtual automatic-teller functionality is provided *only* with respect to the service financial institution, which is supported specifically by the service partner bank. This functionality does *not* extend generally to access other financial institutions that may be connected with the ACH network.

In addition, there is also no motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine Solokl with Newton in the manner suggested by the Office Action. *See* MPEP 2143. The Office Action concedes that there is no disclosure in Solokl of the claim limitations requiring the use of a computer-readable storage medium to access financial accounts, including by decrypting information retrieved from the storage medium. The reference that is relied on instead for these limitations, i.e. Newton, teaches the use of “ultra long identification keys” in providing access to remote computers, and suggests that these long keys may be stored on a CD-ROM (Newton, Col. 2, ll. 35 – 39). The Office Action would like to adapt the authentication mechanism disclosed in Newton to the system of Solokl, offering as the only motivation, “to improve network security by allowing users to enter longer, and hence more secure, identification codes and providing an efficient means for entering the code” (Office Action, p. 4).

This suggestion, however, is not only absent from Solokl, but is also directly contrary to the teachings of Solokl. In particular, Solokl teaches that the actual PIN used to access the financial account be withheld from the user and that a lookup table be used to match a pass phrase to the PIN, indicating that this is used to enhance security (Solokl, Col. 7, l. 54 – 59). While the Office Action would like to do away with such a lookup arrangement and provide the user with the PIN, perhaps in encrypted form, this is directly contrary to the teachings of Solokl that the PIN be withheld to enhance security. Moreover, the motivation provided in the Office Action is unconvincing since Solokl already contemplates the use of a pass phrase that may be used and may be significantly longer than the PIN derived from the lookup table. The use of a pass phrase not only has the advantage that it may be as long as the ultra long identification keys discussed in Newton, but is easily remembered because of its mnemonic character.

The Court of Appeals for the Federal Circuit has repeatedly emphasized the need to apply the requirement that there be a motivation to combine references rigorously, cautioning that such rigor is “the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis.” *In re Dembiczak*, 50 USPQ2d

1614, 1617 (Fed. Circ. 1999). “The need for specificity pervades this authority.” *In re Lee*, 61 USPQ2d 1430, 1433 (Fed Cir. 2002). In this instance, the Examiner’s entirely casual suggestion that longer identification codes could improve security is, at best, nothing more than application of an impermissible hindsight analysis. The proffered reasoning is nonspecific and fails to “explain the reasons one of ordinary skill in the art would have been motivated *to select the references and to combine them* to render the claimed invention obvious.” *In re Rouffet*, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998, emphasis added).

For at least these reasons, the claims of Group 1 are believed to be patentable.

II. Group 2: Patentability of Claims 5 – 8

Each of the claims in Group 2 depends from Claim 1. Accordingly, the arguments set forth with respect to Group 1, namely that some limitations are not disclosed in any of the cited art and that there is no motivation to combine the cited art as the Examiner suggests, are equally applicable to this group of claims.

Furthermore, each of the claims of Group 2 also requires, beyond the limitations of the claims of Group 1, that the decryption processor be “operative to extract a second identifier pertaining to said customer’s financial account from the decrypted information and to re-encrypt the extracted second identifier.” This second identifier is in addition to a first identifier related to the customer’s financial account requested from the customer. The Final Office Action purports to rely on Bocinsky for this limitation, but the specific comments (Final Office Action, ¶5) show that the Examiner is focusing merely on re-encryption of an identifier, ignoring the fact that the claim limitation requires extraction of a *second* identifier that is re-encrypted. It is believed that the failure to cite any portion of Bocinsky requiring *two* identifiers for access to the financial account, one of which is extracted from the decrypted information

and then re-encrypted, is a result of the fact that the limitation is simply not disclosed there.


In addition, the fact that Bocinsky teaches the use of a *single* identifier acts to teach away from the claim limitation requiring *two* identifiers. Such teaching away has long been recognized as a significant factor that indicates that there is in fact *no* motivation to make the combination. The comments in the Final Office Action attempting to establish a motivation are again devoted entirely to the idea that re-encryption of an identifier could increase security of a system, but provide no reasoning to motivate the extraction of a second identifier as the claims require.

As for the claims of Group 1, no *prima facie* case has been established under §103 for the claims of Group 2, neither showing that all limitations are set forth nor providing an adequate motivation to combine teachings from the references relied upon. For these additional reasons, therefore, the claims of Group 2 are also believed to be patentable.

9. Conclusion

Appellant believes that the above discussion is fully responsive to all grounds of rejection set forth in the application. It is believed that no fee is required for filing the Notice of Appeal or this Appeal Brief since such fees have previously been paid in connection with an earlier appeal on which prosecution was reopened prior to a decision on the merits by the Board. Should the Patent Office nevertheless determine that a fee is due, please deduct the requisite fee from Deposit Account 20-1430.

Respectfully submitted,


Patrick M. Boucher
Reg. No. 44,037

Paul Charles Turgeon
Application No.: 09/394,143
Page 11

PATENT

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
PMB:pmb
60089010 v1

APPENDIX

The claims pending in the application are as follows:

1. (Previously Presented) A system for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, at least some of said financial accounts being maintained at different ones of said financial institutions, said system comprising:

for each customer, a network access device including a programmable controller for executing code and a memory for storing a browser software to interface with said public network, said each customer using said network access device and a computer-readable portable storage medium to access said each customer's financial account via said public network, said computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said each customer's financial account; and

a decryption processor, connected to said network access device via said public network, for decrypting said encrypted information retrieved from said storage medium such that the financial institution maintaining said each customer's financial account, connected to said decryption processor via said private network, determines an access to said each customer's financial account on the basis of the decrypted information.

2. (Original) The system according to Claim 1, further comprising a computer connected to said network access device via said public network, said computer hosting a site for goods or services available on-line, said computer comprising a microprocessor being operative to transfer an active module to said network access

device in response to said customer requesting the access to said customer's financial account by using said computer-readable portable storage medium.

3. (Previously Presented) The system according to Claim 2, wherein said active module contains code which is executed by said programmable controller in said network access device such that at least part of said unencrypted information is provided to said customer who is requested to enter a first identifier related to said customer's financial account.

4. (Original) The system according to Claim 3, wherein said programmable controller is operative to transfer the entered first identifier and the encrypted information to said computer for forwarding to said decryption processor.

5. (Original) The system according to Claim 4, wherein said decryption processor is operative to extract a second identifier pertaining to said customer's financial account from the decrypted information and to re-encrypt the extracted second identifier.

6. (Original) The system according to Claim 5, further comprising a network switch located on said private network for routing the re-encrypted second identifier received from said decryption processor to said financial institution maintaining said customer's financial account for determining whether to approve the access to said customer's financial account.

7. (Original) The system according to Claim 6, wherein said financial institution generates a code for indicating whether or not the access to said customer's financial account has been approved and transfers the generated code to said decryption processor via said network switch.

8. (Original) The system according to Claim 7, wherein customer's address data is displayed to said customer on said network access device if said code represents an access approval.

9. (Previously Presented) The system according to Claim 3, wherein the provided unencrypted information includes a name of said financial institution maintaining said customer's financial account.

10. (Previously Presented) The system according to Claim 3, wherein the provided unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

11. (Previously Presented) The system according to Claim 3, wherein the provided unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

12. (Original) The system according to Claim 1, wherein said computer-readable portable storage medium is a CD-ROM.

13. (Original) The system according to Claim 12, wherein said CD-ROM is produced by a card production facility, based on a card production file, for mailing said CD-ROM to said customer.

14. (Original) The system according to Claim 13, wherein said card production file includes an encrypted first identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

15. (Original) The system according to Claim 14, wherein said encrypted first identifier is generated by an encryption module for encrypting a first identifier.

16. (Original) The system according to Claim 15, wherein said first identifier prior to the encryption is generated by a card issuance system which is further operative to generate a second identifier pertaining to said customer's financial account, the generated second identifier being transferred to a mailer production facility for mailing to said customer.

17. (Previously Presented) A method for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, at least some of said financial accounts being maintained at different ones of said financial institutions, said method comprising:

for each customer, accessing said each customer's financial account via said public network using a network access device and a computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said each customer's financial account;

retrieving said encrypted and unencrypted information from said storage medium; and

decrypting the retrieved encrypted information such that the financial institution maintaining said each customer's financial account determines an access to said each customer's financial account on the basis of the decrypted information.

18. (Original) The method according to Claim 17, further comprising using said computer-readable portable storage medium in said network access device in

response to an active module being downloaded to and executed at said network access device such that said unencrypted information is displayed to said customer.

19. (Original) The method according to Claim 18, further comprising entering an identifier pertaining to said customer's financial account in response to the executed active module.

20. (Original) The method according to Claim 19, wherein said unencrypted information includes a name of said financial institution maintaining said customer's financial account.

21. (Original) The method according to Claim 19, wherein said unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

22. (Original) The method according to Claim 19, wherein said unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

23. (Original) The method according to Claim 17, wherein said computer-readable portable storage medium is a CD-ROM.

24. (Original) The method according to Claim 23, wherein said CD-ROM is produced on the basis of a card production file that includes an encrypted identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

25. (Original) The method according to Claim 17, further comprising reviewing customer's address data displayed on a monitor of said network access device if said financial institution has approved the access to said customer's financial account.

26. – 28. (Canceled).